This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Alt-N MDaemon 7.2, **6.8.0-6.8.5**	A vulnerability exists due to a failure to properly drop privileges prior to executing child process, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Alt-N MDaemon Privilege Escalation	Medium	SecurityFocus, November 23, 2004 **SecurityFocus, November 30, 2004**

Burut Creative Team Burut Kreed 1.5	Multiple vulnerabilities exist: a format string vulnerability exists, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability exists when a malicious user submits a large UDP datagram; and a remote Denial of Service vulnerability exists when a malicious nickname or model type is submitted. No workaround or patch available at time of publishing. An exploit script has been published.	Burut Kreed Game Server Multiple Remote Vulnerabilities	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA13361, December 3, 2004
Cisco Systems CNS Network Registrar 6.0-6.0.5 .4, 6.1-6.1.1 .3	Multiple remote Denial of Service vulnerabilities exist in the Domain Name Service and Dynamic Host Configuration Protocol server components when a malicious user submits a specially crafted packet sequence. Updates available at: http://www.cisco.com/pcgi-bin/Software/Tablebuild/tablebuild.pl/nr-eval Currently we are not aware of any exploits for this vulnerability.	Cisco CNS Network Registrar DNS & DHCP Server Remote Denial of Service	Low	Cisco Security Advisory, cisco-sa-20041202, December 2, 2004
Computer Associates Unicenter Remote Control English 6.0 SP1 (Build 6.0.77), GA 6.0 (6.0.56.3), QO48974 6.0 (Build 6.0.74), Unicenter Remote Control French 6.0 SP1 (Build 6.0.77), GA 6.0 (Build 6.0.74), Unicenter Remote Control German 6.0 SP1 (Build 6.0.77), GA 6.0 (Build 6.0.74)	A vulnerability exists due to an unspecified error in the URC Management Console, which could let a remote malicious user obtain unauthorized administrative access. There is no exploit code required. Currently we are not aware of any exploits for this vulnerability.	Computer Associates Unicenter Remote Control Remote Authentication Bypass	High	SecurityFocus, December 3, 2004
David Harris Mercury (win32 version) 4.0 1a	Multiple stack-based buffer overflow vulnerabilities exist in the IMAP server implementation due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. Update available at: ftp://ftp.usm.maine.edu/pegasus/mercury32/m32-401b.zip Exploit scripts have been published.	Mercury Mail Multiple Remote IMAP Stack Buffer Overflows	High	Bugtraq, December 1, 2004
GlobalSCAPE, Inc. CuteFTP 6.0	Multiple buffer overflow vulnerabilities exist in the command and response functionality due to insufficient validation of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GlobalScape CuteFTP Multiple Command Response Buffer Overflow	Low/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1012366, November 30, 2004
Headlight Software, Inc. GetRight 5.2a & prior	A buffer overflow vulnerability exists in the 'DUNZIP32.DLL' component when a specially crafted skin file is created, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GetRight 'DUNZIP32.DLL' Buffer Overflow	High	Secunia Advisory, SA13391, December 7, 2004
HostingController Hosting Controller v.6.1 Hotfix 1.4	Several vulnerabilities exist: a vulnerability exists in 'Statsbrowse.asp' due to a flaw that lets remote malicious users view arbitrary directories; and a vulnerability exists in 'Generalbrowser.asp' due to a flaw that lets remote malicious user view arbitrary files. The vendor has released a patch. Proofs of Concept exploits have been published.	Hosting Controller 'Statsbrowse.asp' & 'Generalbrowse.asp' Information Disclosure	Medium	SecurityTracker Alert ID, 1012426, December 5, 2004
IBEX Software Remote Execute 2.x	A remote Denial of Service vulnerability exists due to an error in the connection handling. Update available at: http://www.ibexsoftware.com/downloadRemoteExecute.asp Currently we are not aware of any exploits for this vulnerability.	IBEX Software Remote Execute Denial of Service	Low	SecurityTracker Alert, 1012445, December 7, 2004
IpSwitch WS_FTP Server 5.03, 2004.10.14	Several vulnerabilities were reported that could permit a remote authenticated malicious user to execute arbitrary code on the target system. A remote authenticated user can trigger a buffer overflow in several FTP commands. The SITE, XMKD, MKD, and RFNR FTP commands are affected. A remote user can cause the FTP service to crash or execute arbitrary code. No workaround or patch available at time of publishing. **Exploit scripts have been published.**	IpSwitch WS_FTP Buffer Overflow	High	SecurityTracker Alert ID: 1012353, November 29, 2004 **SecurityFocus, November 30, 2004**
Microsoft Windows 2000/XP Resource Kit	Several vulnerabilities exist in the 'w3who.dll' Microsoft ISAPI extension in the Windows 2000/XP Resource Kit: Cross-Site Scripting vulnerabilities exist when displaying HTTP headers and in error messages, which could let a remote malicious user execute arbitrary HTML and script code; and a buffer overflow vulnerability exists when processing input parameters, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Microsoft Windows Resource Kit 'w3who.dll' Buffer Overflow & Input Validation CVE Names: CAN-2004-1133 CAN-2004-1134	High	Exaprobe Security Advisory, December 6, 2004

Microsoft ISA Server 2000, Proxy Server 2.0	A spoofing vulnerability exists that could enable a malicious user to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious web site. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms04-039.mspx V2.0 (November 9, 2004): Bulletin updated to reflect the release of an updated ISA Server 2000 security update for the German language only. This issue does not affect any other language version of this security update. The Security Update Replacement section has also been revised. V3.0 (November 16, 2004): Bulletin updated to reflect the release of updated ISA Server 2000 security updates for all languages. These issues affected customers using ISA Server 2000 Service Pack 1 or using Windows 2000 Service Pack 3. The Security Update Replacement section has also been revised. Microsoft Security Bulletin updated to reflect a revised Security Update Information section for the Proxy 2.0 Service Pack 1 security update. **V3.2: Bulletin updated to reflect a revised Security Update Information section for the Proxy 2.0 Service Pack 1 security update. This update documents that the Proxy 2.0 Service Pack 1 security update uses local date and time information instead of UTC date and time information.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Server Spoofing CVE Name: CAN-2004-0892	Medium	Microsoft Security Bulletin, MS04-039 2.0, 3.0, 3.1, November 19, 2004 (Updated) **Microsoft Security Bulletin, MS04-039 Rev 3.2, November 30, 2004**
Microsoft Internet Explorer 6	A vulnerability exists when processing FTP URLs, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer FTP URL Processing Input Validation	High	7a69ezine Advisories , December 7, 2004
Microsoft Internet Explorer 6.0 SP1, Microsoft Internet Explorer 6.0	A remote buffer overflow vulnerability exists due to insufficient boundary checks performed by the application and results in a Denial of Service condition. Arbitrary code execution may be possible as well. **Patches available at:** **http://www.microsoft.com/technet/security/bulletin/ms04-040.mspx** ***Note: Customers who have received hotfixes from Microsoft or from their support providers since the release of MS04-004 or MS04-038 should not install this update. Instead customers should deploy update 889669.*** ***Microsoft Knowledge Base Article 889293 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues.*** An exploit script has been published.	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow CVE Name: CAN-2004-1050	Low/High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID 11515, October 25, 2004 Packetstorm, November 4, 2004 **Microsoft Security Bulletin, MS04-040, December 1, 2004** **Technical Cyber Security Alert, TA04-336A, December 3, 2004**
Microsoft Internet Explorer 6.0, SP1&2, Windows XP 64-bit Edition SP1 Windows XP 64-bit Edition, 64-bit Edition Version 2003, SP1, XP Embedded, SP1, XP Home, SP1&2, XP Media Center Edition, SP1&2, XP Professional, SP1&2, XP Tablet PC Edition	A vulnerability exists which could let a remote malicious user execute arbitrary HTML and script code if a maliciously constructed file were 'dragged and dropped.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Drag & Drop	High	SecurityFocus, November 29, 2004
Microsoft Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6.0 for Windows Server 2003, Internet Explorer 6.0 for Windows XP Service Pack 2, Windows 98, Windows 98 SE, Windows ME, Internet Explorer 5.5; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-038. These vulnerabilities include: Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability; Similar Method Name Redirection Cross Domain Vulnerability; Install Engine Vulnerability; Drag and Drop Vulnerability; Address Bar Spoofing on Double Byte Character Set Locale Vulnerability; Plug-in Navigation Address Bar Spoofing Vulnerability; Script in Image Tag File Download Vulnerability; SSL Caching Vulnerability. These vulnerabilities could allow remote code execution. A vulnerability exists in the Microsoft MSN 'heartbeat.ocx' component, used by Internet Explorer on some MSN gaming sites Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() Updated the ActiveX control name from "Heartbeat.ocx" to "Hrtbeat.ocx", added GUID information to the Security Update Information section.	Microsoft Internet Explorer Security Update CVE Names: CAN-2004-0842 CAN-2004-0727 CAN-2004-0216 CAN-2004-0839 CAN-2004-0844 CAN-2004-0843 CAN-2004-0841 CAN-2004-0845	High	Microsoft Security Bulletin, MS04-038, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Notes VU#637760, October 13, 2004, VU#625616, October 15, 2004, VU#431576, VU#630720, & VU#291304, October 18, 2004, VU#673134 & VU#795720, October 19, 2004 SecurityFocus, October 18, 2004 Microsoft Security Bulletin, MS04-038, November 9, 2004 **SecurityFocus, November 29, 2004**

	A Proof of Concept exploit has been published.			
Microsoft Small Business Server 2000, 2003, Windows 2000 Advanced Server , SP1-SP4, Windows 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, Windows Server 2003 Datacenter Edition, 64-bit, Server 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition	A buffer overflow vulnerability exists in the Microsoft Windows Internet Name Service (WINS), which could let a remote malicious user execute arbitrary code with SYSTEM level privileges. Workaround available at: http://support.microsoft.com/kb/890710 There is no exploit circulating at this time.	Microsoft Windows WINS Buffer Overflow	High	SecurityFocus, November 30, 2004 US-CERT Vulnerability Note VU#145134, December 6, 2004
Thomas Hauck JanaServer 2 2.4.0-2.4.4	Two vulnerabilities exist: a remote Denial of Service vulnerability exists in the'http-server' module when a malicious user submits a specially crafted HTTP request that contains a large of '%' characters to port 2506; and a remote Denial of Service vulnerability exists in the 'pna-proxy' module when handling Real Player requests. Updates available at: http://www.janaserver.de/start.php?lang=en&menue=download&content=down An exploit script has been published.	JanaServer 2 Multiple Remote Denial of Service	Low	Bugtraq, November 30, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.50	A remote Denial of Service vulnerability exists in Apache 2 mod_ssl during SSL connections. Apache: http://nagoya.apache.org/bugzilla/show_bug.cgi?id=29964 RedHat: http://rhn.redhat.com/errata/RHSA-2004-349.html SUSE: ftp://ftp.SUSE.com/pub/SUSE/i386/update/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ HP: http://software.hp.com **Apple:** **http://www.apple.com/swupdates/** Currently we are not aware of any exploits for this vulnerability.	Apache mod_ssl Denial of Service CVE Name: CAN-2004-0748	Low	SecurityFocus, September 6, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004 Gentoo Linux Security Advisory, GLSA 200409-21, September 16, 2004 Trustix Secure Linux Security Advisory,TSLSA-2004-0047, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004 Fedora Update Notification, FEDORA-2004-313, September 23, 2004 HP Security Bulletin, HPSBUX01090, October 26, 2004 **Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004**
Apache Software Foundation Apache 2.0.50	A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126 SUSE: ftp://ftp.SUSE.com/pub/SUSE/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-463.html	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0751	Low	SecurityTracker Alert ID, 1011213, September 10, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004 RedHat Security Advisory, RHSA-2004:463-09, September 15, 2004 Gentoo Linux Security Advisory GLSA 200409-21, September 16, 2004

	Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml Trustix: http://www.trustix.org/errata/2004/0047/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ HP: http://h30097.www3.hp.com/internet/download.htm **Apple:** **http://www.apple.com/swupdates/** There is no exploit code required; however, Proofs of Concept exploits have been published.			Trustix Secure Linux Security Advisory , TSLSA-2004-0047, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004 Fedora Update Notification, FEDORA-2004-313, September 23, 2004 HP Security Bulletin, HPSBUX01090 & HPSBGN01091, October 26 & 29, 2004 **Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004**
Apache Software Foundation Conectiva Gentoo HP Immunix Mandrake OpenBSD OpenPKG RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD –current, 3.4, 3.5	A buffer overflow vulnerability exists in Apache mod_proxy when a 'ContentLength:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200406-16.xml Mandrake: http://www.mandrakesoft.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Apple:** **http://www.apple.com/swupdates/** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_Proxy Remote Buffer Overflow CVE Name: CAN-2004-0492	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1010462, June 10, 2004 Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:065, June 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004 SGI Security Advisory, 20040605-01-U, June 21, 2004 Fedora Legacy Update Advisory, FLSA:1737, October 14, 2004 US-Cert Vulnerability Note VU#541310, October 19, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004 Turbolinux Security Announcement, November 18, 2004 **Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004**
Apple Mac OS X 10.2.8 Client Mac OS X 10.2.8 Server Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability was reported in Apache running on an Apple HFS+ filesystem. A remote malicious user may be able to directly access file data or resource fork contents. Apple reported that a remote user can supply a specially crafted HTTP request to bypass the Apache file handler and directly access certain content using the special file names. The Apple HFS+ filesystem permits files to have multiple data streams and be access via special filenames. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Apache File Handlers Bypass & Directly Access CVE Name: CAN-2004-1084	Medium	Apple Security Update, December 2, 2004
Apple Mac OS X 10.2.8 Client Mac OS X 10.2.8 Server Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability was reported in Apache when running on Mac OS X with the Apple HFS+ filesystem. A remote malicious user may be able to gain access to certain files on the system. Apple reported that the web server configuration does not properly block access to '.DS_Store' files and files that start with the string '.ht'. The web server operates in a case sensitive manner but the HFS+ filesystem is case insensitive. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Apache on Apple HFS+ '.DS_Store' Files Disclosure CVE Name: CAN-2004-1083	Medium	Apple Security Update, December 2, 2004

Apple Mac OS X 10.2.8 Client Mac OS X 10.2.8 Server Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability was reported in Apple's AppKit. One application may be able to access ostensibly secure data from another application in the same window. The vendor reported that in some cases, secure input is not properly enabled. As a result, an application may be able to read characters entered into a secure text field of another window in that session. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple AppKit Secure Input CVE Name: CAN-2004-1081	Medium	Apple Security Update, December 2, 2004
Apple Mac OS X 10.2.8 Client Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability exists in the Cyrus IMAP server when used with Kerberos authentication, affecting Mac OS X and possibly other operating systems which could allow a remote authenticated malicious user to gain access to another mailbox on the target system. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Cyrus IMAP Server Remote Mailbox Access CVE Name: CAN-2004-1089	Medium	Apple Security Update, December 2, 2004
Apple Mac OS X 10.2.8 Server Mac OS X 10.3.6 Server	A vulnerability was reported in Apache mod_digest_apple. A remote malicious user can replay previously recorded authentication credentials. Apple reported that that a remote user may be able to exploit this flaw to gain access to the target web service. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Apache mod_digest_apple Authentication Credentials Replay CVE Name: CAN-2004-1082	Medium	Apple Security Update, December 2, 2004
Apple Mac OS X 10.2.8 Server Mac OS X 10.3.6 Server	A vulnerability exists in Apples's QuickTime Streaming Server. A remote malicious user can cause Denial of Service conditions. Apple reported that a remote user can send specially crafted DESCRIBE requests to the target streaming server to cause Denial of Service conditions. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple QuickTime Streaming Server Remote Denial of Service CVE Name: CAN-2004-1123	Low	Apple Security Update, December 2, 2004
Apple Mac OS X 10.3.6 Client; Mac OS X 10.3.6 Server	A vulnerability exists in HIToolbox that could allow a physically local malicious user to quit applications with a special key combination when in kiosk mode. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple HIToolbox Kiosk Mode Application Quit CVE Name: CAN-2004-1085	Low	Apple Security Update, December 2, 2004
Apple Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability exists in Postfix when using CRAM-MD5 authentication. A remote malicious user may be able to send mail via the target system. Apple reported that in some situations, a remote user may be able to replay previously recorded CRAM-MD5 authentication credentials during a small time period to send mail via the system. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Postfix CRAM-MD5 Replay Attack CVE Name: CAN-2004-1088	Medium	Apple Security Update, December 2, 2004
Apple Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability exists in PSNormalizer in the conversion of PostScript files to PDF format that could allow a remote malicious user to execute arbitrary code. Apple reported that a remote user can create a specially crafted PostScript document that, when converted by the target user, will execute arbitrary code with the privileges of the target user. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple PSNormalizer Buffer Overflow CVE Name: CAN-2004-1086	High	Apple Security Update, December 2, 2004
Apple Mac OS X 10.3.6 Client Mac OS X 10.3.6 Server	A vulnerability exists in Mac OS X Terminal. The terminal may display the incorrect 'Secure Keyboard Entry'. The vendor reported that the 'Secure Keyboard Entry' menu setting may be displayed when it is not active. Apple has issued a fix as part of Security Update 2004-12-02, available at: http://www.apple.com/swupdates/ Currently we are not aware of any exploits for this vulnerability.	Apple Terminal Incorrect 'Secure Keyboard Entry' Status CVE Name: CAN-2004-1087	Low	Apple Security Update, December 2, 2004
Caolan McNamara & Dom Lachowicz wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0	A buffer overflow vulnerability exists in the 'strcat()' function call due to the insecure bounds checking, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root =/cvsroot&file=field.c&rev1=1.19&rev2=1.20 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-11.xml	wvWare Library Buffer Overflow CVE Name: CAN-2004-0645	High	Securiteam, July 11, 2004 iDEFENSE Security Advisory, July 9, 2004 Conectiva Linux Security Announcement, CLA-2004:863, September 10, 2004 Debian Security Advisory, DSA 550-1, September 20, 2004 Debian Security Advisory, DSA 579-1, November 1, 2004

	Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/w/wv/ A Proof of Concept exploit has been published.			**Conectiva Linux Security Announcement, CLA-2004:902, December 1, 2004**
Carsten Haitzler imlib 1.x	Multiple vulnerabilities exist due to integer overflows within the image decoding routines. This can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library. Gentoo: http://security.gentoo.org/glsa/glsa-200412-03.xml Currently we are not aware of any exploits for these vulnerabilities.	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026	High	Secunia Advisory ID: SA13381, December 7, 2004
Debian Debian GNU/Linux 3.0, Debian GNU/Linux unstable alias sid	A vulnerability exists in hpsockd, which can be exploited by malicious people to cause a Denial of Service and potentially compromise a vulnerable system. The vulnerability is caused due to an unspecified boundary error, which can be exploited to cause a buffer overflow. Updates available: http://www.debian.org/security/2004/dsa-604 Currently we are not aware of any exploits for this vulnerability.	Debian hpsockd Buffer Overflow Vulnerability	Low/High (High if arbitrary code can be executed)	Debian Security Advisory DSA-604-1, December 2, 2004
Dom Lachowicz AbiWord 2.0.7 and prior	A vulnerability exists in the "wv" library of AbiWord, which could be exploited by an attacker to compromise a user's system. Update to version 2.0.8 or later available at: http://www.abisource.com/download/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000902** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Dom Lachowicz AbiWord "wv" Library Buffer Overflow	High	AbiWord 2.0.7-2.0.9 Changes Secunia, SA12136 and SA12146, July 26, 2004 Secunia Advisory ID: SA13344, December 2, 2004 **SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004**
Downhill Battle Blog Torrent Preview Version 0.8	A vulnerability exists that could permit a remote malicious user to view files on the target system. The 'btdownload.php' script does not properly validate user-supplied input in the 'file' parameter. A remote user can submit a specially crafted URL to traverse the directory and view arbitrary files with the privileges of the target web service. A fix is available via CVS at: http://cvs.sourceforge.net/viewcvs.py/battletorrent/btorrent_server/btdownload.php?r1=1.6&r2=1.7 A Proof of Concept exploit has been published.	Downhill Battle Blog Torrent 'btdownload.php' Input Validation	Medium	SecurityTracker Alert ID: 1012390, December 2, 2004
Federico D. Sacerdoti Ansel 2.1	Multiple vulnerabilities exist which can be exploited by malicious people to conduct SQL injection and script insertion attacks. Input passed to the "image" parameter is not properly sanitized before being used in a SQL query. Also, input passed to the album name field is not properly sanitized before being used. Update to version 2.2: ftp://heron.sdsc.edu/pub/ansel-2.2.tar.gz Currently we are not aware of any exploits for these vulnerabilities.	Federico D. Sacerdoti Ansel "image" SQL Injection & Script Insertion	High	Secunia Advisory ID: SA12856, December 6, 2004
FreeBSD Project FreeBSD Kernel	A vulnerability exists in the kernel which can be exploited by malicious, local users to gain knowledge of sensitive information or cause a Denial of Service. The vulnerability is caused due to an error in "/proc/curproc/cmdline" of the procfs file system and "/proc/self/cmdline" of the linprocfs file system when reading an argument vector from a process address space. This can be exploited to disclose parts of kernel memory or crash a vulnerable system. Successful exploitation requires that the procfs or linprocfs file system is mounted. Patches available: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04%3A17.procfs.asc Currently we are not aware of any exploits for this vulnerability.	FreeBSD Kernel Memory Disclosure CVE Name: CAN-2004-1066	Medium	FreeBSD-SA-04:17 Security Advisory, December 1, 2004

GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml Debian: http://security.debian.org/pool/updates/main/libg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/updates/main/libg/libgd/** An exploit script has been published.	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990	High	Secunia Advisory, SA12996, October 28, 2004 Gentoo Linux Security Advisory, GLSA 200411-08, November 3, 2004 Ubuntu Security Notice, USN-21-1, November 9, 2004 Debian Security Advisories, DSA 589-1 & 591-1, November 9, 2004 Fedora Update Notifications, FEDORA-2004-411 & 412, November 11, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:132, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-25-1, November 16, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 **Debian Security Advisories, DSA 601-1 & 602-1, November 29, 2004**
Gentoo mirrorselect-0.88 and prior	A vulnerability exists in mirrorselect, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.The vulnerability is caused due to temporary files being created insecurely. This can be exploited via symlink attacks to overwrite arbitrary files on the system with the privileges of the user executing the mirrorselect tool. Update to "app-portage/mirrorselect-0.89" or later: http://security.gentoo.org/glsa/glsa-200412-05.xml Currently we are not aware of any exploits for this vulnerability.	Gentoo mirrorselect Insecure Temporary File Creation	Medium	Gentoo Security Advisory, GLSA 200412-05 / mirrorselect, December 7, 2004
Gentoo PDFlib	Multiple overflow vulnerabilities exists in PDFlib which can be exploited by malicious people to execute arbitrary code or cause a Denial of Service. Update to "media-libs/pdflib-5.0.4_p1" or later available at: http://security.gentoo.org/glsa/glsa-200412-02.xml Currently we are not aware of any exploits for this vulnerability.	Gentoo PDFlib Buffer Overflow	High	Gentoo Linux Security Advisory, GLSA 200412-02 / PDFlib, December 2, 2004
Gentoo perl	Multiple vulnerabilities exist which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. A local attacker could create symbolic links in the temporary files directory, pointing to a valid file somewhere on the filesystem. When a Perl script is executed, this would result in the file being overwritten with the rights of the user running the utility, which could be the root user. Update to "perl-5.8.5-r2" or later: http://security.gentoo.org/glsa/glsa-200412-04.xml Currently we are not aware of any exploits for these vulnerabilities.	Gentoo Perl Privilege Escalation	Medium	Gentoo Security Advisory, GLSA 200412-04 / perl, December 7, 2004
Global Moxie Big Medium 1.0	A vulnerability exists due to an unspecified error, which could let a remote malicious user execute arbitrary code. Update available at: http://www.globalmoxie.com/cgi-bin/license/download.cgi Currently we are not aware of any exploits for this vulnerability.	Global Moxie Big Medium Remote Script Code Execution	High	SecurityFocus, December 2, 2004
IBM AIX 5.1, 5.2, 5.3	A vulnerability has been reported in AIX, which can be exploited by malicious, local users to inject arbitrary data into the ODM (Object Data Manager) or cause a vulnerable system to hang during boot.The vulnerability is caused due to an unspecified error within the system startup scripts. Apply APARs: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp Currently we are not aware of any exploits for this vulnerability.	IBM AIX Unspecified System Startup Scripts	Low	SecurityTracker Alert ID: 1012419, December 3, 2004
ImageMagick ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8,	A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at:	ImageMagick Remote EXIF Parsing Buffer	High	SecurityTracker Alert ID, 1011946, October 26, 2004 Gentoo Linux Security

5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8	http://sourceforge.net/project/showfiles.php?group_id=24099 Redhat: http://rhn.redhat.com/errata/RHSA-2004-480.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-11.xml Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ SUSE: ftp://ftp.SUSE.com/pub/SUSE/i386/update/ **Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:143** Currently we are not aware of any exploits for this vulnerability.	Overflow CVE Name: CAN-2004-0981		Advisory, GLSA 200411-11:01, November 6, 2004 Debian Security Advisory DSA 593-1, November 16, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 SUSE Security Summary Report, USE-SR:2004:001, November 24, 2004 **Mandrakesoft Security Advisory, MDKSA-2004:143, December 6, 2004**
KDE KDE Konqueror 3.3.1 and prior	A vulnerability exists in the processing of FTP URLs that could allow a remote malicious user to cause FTP commands to be executed. A remote user can create a specially crafted FTP URL that, when loaded by the target user, will execute arbitrary FTP commands on the specified FTP server. The commands can be appended to the URL, separated by the string '%0a'. The target user must first be authenticated against the FTP server for the exploit to work. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	KDE Konqueror Input Validation	High	SecurityTracker Alert ID: 1012443, December 7, 2004
libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Proofs of Concept exploits have been published.	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004 Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 **US-CERT Vulnerability Notes VU#687568 & VU#948752, December 1, 2004**

Multiple Vendors
Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64;
RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core1&2;
Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1;
Turbolinux Turbolinux Desktop 10.0
	A buffer overflow vulnerability exists in the apr-util library's IPv6 URI parsing functionality due to insufficient validation, which could let a remote malicious user execute arbitrary code. *Note: On Linux based Unix variants this issue can only be exploited to trigger a Denial of Service condition.*
	Patch available at:
	http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch
	Gentoo:
	http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Redhat:
	http://rhn.redhat.com/errata/RHSA-2004-463.html
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	Trustix:
	ftp://ftp.trustix.org/pub/trustix/updates/
	TurboLinux:
	ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	HP:
	http://h30097.www3.hp.com/internet/download.htm
	Apple:
	http://www.apple.com/swupdates/
	Current y we are not aware of any exploits for this vulnerability.
		Apache Web Server Remote IPv6 Buffer Overflow
		CVE Name:
		CAN-2004-0786
			Low/High
			(High if arbitrary code can be executed)
				SecurityFocus, September 16, 2004
				Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004
				Fedora Update Notifications, FEDORA-2004-307 & 308, September 16, 2004
				HP Security Bulletin, HPSBUX01090 & HPSBGN01091, October 26 & 29, 2004
				Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004

Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.1.7, 2.1.9, 2.1.10, 2.1.16, 2.2 .0 ALPHA, 2.2.1 BETA, 2.2.2 BETA, 2.2.3-2.2.8; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PROXY' and 'LOGIN' commands if the 'IMAPMAGICPLUS' option is enabled, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument parser for the 'PARTIAL' command, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument handler for the 'FETCH' command, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handler for the 'APPEND' command, which could let a remote malicious user execute arbitrary code. Carnegie Mellon University: ftp://ftp.andrew.cmu.edu/pub/cyrus/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-imapd/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **OpenPKG:** **ftp://ftp.openpkg.org/release/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE/** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAPD Multiple Remote Vulnerabilities CVE Names: CAN-2004-1011 CAN-2004-1012 CAN-2004-1013	High	Securiteam, November 23, 2004 Debian Security Advisory, DSA 597-1, November 25, 2004 Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 Trustix Secure Linux Advisory, TSL-2004-0063. November 29, 2004 **OpenPKG Security Advisory, OpenPKG-SA-2004.051, November 29, 2004** **Conectiva Linux Security Announcement, CLA-2004:904, December 1, 2004** **Fedora Update Notifications, FEDORA-2004-487 & 489, December 1, 2004** **SUSE Security Announcement, SUSE-SA:2004:043, December 3, 2004**

Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.2.9 & prior	A buffer overflow vulnerability exists in the 'imap magic plus' support code, which could let a remote malicious user execute arbitrary code. Update available at: http://asg.web.cmu.edu/cyrus/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/** **Conectiva:** **http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000904** **SUSE:** **ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Cyrus IMAP 'imap magic plus' Buffer Overflow CVE Name: CAN-2004-1015	High	Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 **Secunia SA13349, December 2, 2004** **Secunia Advisory ID: SA13346, December 2, 2004** **Secunia Advisory ID: 13366, December 6, 2004**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, 0 ia-64, ia-32, hppa, arm, alpha; Linux kernel 2.0.2, 2.4-2.4.26, 2.6-2.6.9	A vulnerability exists in 'iptables.c' and 'ip6tables.c' due to a failure to load the required modules, which could lead to a false sense of security because firewall rules may not always be loaded. Debian: http://security.debian.org/pool/updates/main/i/iptables/i Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/** **SUSE:** **ftp.SUSE.com/pub/SUSE** There is no exploit code required.	IpTables Initialization Failure CVE Name: CAN-2004-0986	Medium	Debian Security Advisory, DSA 580-1 , November 1, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:125, November 4, 2004 **SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004** **Fedora Update Notification, FEDORA-2004-417, December 1, 2004**
Multiple Vendors GD Graphics Library gdlib 1.8.4, 2.0.1, 2.0.20-2.0.23, 2.0.26-2.0.28	Multiple buffer overflow vulnerabilities exist due to insufficient bounds checking prior to processing user-supplied strings, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Debian:** **http://security.debian.org/pool/updates/main/libg/** Currently we are not aware of any exploits for these vulnerabilities.	GD Graphics Library Multiple Remote Buffer Overflows CVE Name: CAN-2004-0941	High	SecurityTracker, 1012195, November 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 **Debian Security Advisories, DSA 601-1 & 601-2, November 29, 2004**
Multiple Vendors gzip	A vulnerability exists in the gzip(1) command, which could let a malicious user access the files of other users that were processed using gzip. Sun Solaris: http://sunsolve.sun.com/search/ document.do?assetkey=1-26-57600-1 **Mandrakesoft:** **http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:142** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Gzip File Access	Medium	Sun(sm) Alert Notification, 57600, October 1, 2004 US-CERT Vulnerability Note VU#635998, October 18, 2004 **Mandrakesoft Security Advisory, MDKSA-2004:142, December 6, 2004**
Multiple Vendors nfs-utils 1.0.6	A vulnerability exists due to an error in the NFS statd server in "statd.c" where the "SIGPIPE" signal is not correctly ignored. This can be exploited to crash a vulnerable service via a malicious peer terminating a TCP connection prematurely. Upgrade to 1.0.7-pre1: http://sourceforge.net/project/ showfiles.php?group_id=14&package_id=174 Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:146 Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors nfs-utils "SIGPIPE" TCP Connection Termination Denial of Service	Low	Secunia Advisory ID: SA13384, December 7, 2004
Multiple Vendors OpenSSH 3.0 p1-3.0.2 pl1, 3.0-3.0.2, 3.1-3.5, 3.1pl1, 3.2.2 p1, 3.2.3 p1, 3.3 p1-3.5pl1, 3.6.1 p1&pl2, 3.6.1, 3.7, 3.7.1, 3.7	An information disclosure vulnerability exists in the portable version of OpenSSH that is distributed for operating systems other than its native OpenBSD platform, which could let a remote malicious user obtain sensitive information. Ubuntu:	OpenSSH-portable Remote Information Disclosure CVE Name:	Medium	Ubuntu Security Notice, USN-34-1 November 30, 2004

p1&pl2, 3.7.1 p1, 3.8.1 p1, 3.9.1 pl1	http://security.ubuntu.com/ubuntu/pool/main/o/openssh/ There is no exploit code required.	CAN-2003-0190		
Multiple Vendors Cisco VPN 3000 Concentrator 4.0 .x, 4.0, 4.0.1, 4.1 .x; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.4 _rc1-rc3, 1.4; MandrakeSoft Corporate Server 2.1, x86_64, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64, MandrakeSoft Multi Network Firewall 8.2; MIT Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2-1.2.8, 1.3 -1.3.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core2, Core1; Sun SEAM 1.0.2	Multiple double-free vulnerabilities exist due to inconsistent memory handling routines in the krb5 library: various double-free errors exist in the KDC (Key Distribution Center) cleanup code and in client libraries, which could let a remote malicious user execute arbitrary code; various double-free errors exist in the 'krb5_rd_cred()' function, which could let a remote malicious user execute arbitrary code; a double-free vulnerability exists in krb524d, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in ASN.1 decoder when handling indefinite length BER encodings, which could let a remote malicious user cause a Denial of Service. MIT Kerberos: http://web.mit.edu/kerberos/advisories/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-09.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-21-112908-15-1 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860 OpenPKG: ftp://ftp.openpkg.org/release/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ IBM: http://www.securityfocus.com/advisories/7269 **Apple:** **http://www.apple.com/swupdates/** Currently we are not aware of any exploits for these vulnerabilities.	Kerberos 5 Double-Free Vulnerabilities CVE Names: CAN-2004-0642 CAN-2004-0643 CAN-2004-0772	Low/High (High if arbitrary code can be executed)	MIT krb5 Security Advisory, MITKRB5-SA-2004-002, August 31, 2004 US-CERT Technical Cyber Security Alert TA04-247A, September 5, 2004 US-CERT Vulnerability Notes, VU#350792, VU#795632, VU#866472, September 3, 2004 Conectiva Security Advisory, CLSA-2004:860, September 9, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.039, September 13, 2004 Turbolinux Security Advisory TLSA-2004-22, September 15, 2004 IBM Security Advisory, September 30, 2004 **Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004**
Multiple Vendors Cisco VPN 3000 Concentrator 4.0 .x, 4.0, 4.0.1, 4.1 .x; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.4 _rc1-rc3, 1.4; MandrakeSoft Corporate Server 2.1, x86_64, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64, MandrakeSoft Multi Network Firewall 8.2; MIT Kerberos 5 1.2.2-1.2.8, 1.3 -1.3.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core2, Core1; Sun Solaris 9.0, 9.0 _x86	A remote Denial of Service vulnerability exists in the ASN.1 decoder when decoding a malformed ASN.1 buffer. MIT Kerberos: http://web.mit.edu/kerberos/advisories/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-09.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57631-1&searchclause= Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860 OpenPKG: ftp://ftp.openpkg.org/release/	MIT Kerberos 5 ASN.1 Decoder Remote Denial of Service CVE Name: CAN-2004-0644	Low	MIT krb5 Security Advisory, MITKRB5-SA-2004-002, August 31, 2004 US-CERT Technical Cyber Security Alert TA04-247A, September 5, 2004 US-CERT Vulnerability Note VU#550464, September 3, 2004 Conectiva Security Advisory, CLSA-2004:860, September 9, 2004 OpenPKG Security Advisory , OpenPKG-SA-2004.039, September 13, 2004 Turbolinux Security Advisory TLSA-2004-22, September 15, 2004 **Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004**

	TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ **Apple:** **http://www.apple.com/swupdates/** Currently we are not aware of any exploits for this vulnerability.			

Multiple Vendors
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;
Gentoo Linux;
GNOME GPdf 0.112;
KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2;
RedHat Fedora Core2;
Ubuntu ubuntu 4.1, ppc, ia64, ia32,
Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0, SUSE Linux - all versions
	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.
	Debian:
	http://security.debian.org/pool/updates/main/c/cupsys/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200410-20.xml
	KDE:
	ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Debian:
	http://security.debian.org/pool/updates/main/t/tetex-bin/
	SUSE: Update:
	ftp://ftp.SUSE.com/pub/SUSE
	Currently we are not aware of any exploits for these vulnerabilities.
		Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows
		CVE Names:
		CAN-2004-0888
		CAN-2004-0889
			High	SecurityTracker Alert ID, 1011865, October 21, 2004
				Conectiva Linux Security Announcement, CLA-2004:886, November 8, 2004
				Debian Security Advisory, DSA 599-1, November 25, 2004
				SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004

Multiple Vendors
Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1;
ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0- 2003040, 5.5.7,6.0.2;
Imlib Imlib 1.9-1.9.14
	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.
	Imlib:
	http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/
	ImageMagick:
	http://www.imagemagick.org/www/download.html
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200409-12.xml
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/main/i/imagemagick/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2004-465.html
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE/
	TurboLinux:
	ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Sun:
	http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause=
	http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause=
	TurboLinux:
	ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/
	RedHat:
		IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows
		CVE Names:
		CAN-2004-0817
		CAN-2004-0802
			Low/High
			(High if arbitrary code can be executed)
				SecurityFocus, September 1, 2004
				Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004
				Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004
				Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004
				Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004
				RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004
				Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004
				Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004
				Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004
				Turbolinux Security Announcement, October 5, 2004
				RedHat Security Update, RHSA-2004:480-05, October 20, 2004
				Ubuntu Security Notice USN-35-1, November 30, 2004

	http://rhn.redhat.com/errata/RHSA-2004-480.html **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/i** Currently we are not aware of any exploits for these vulnerabilities.			

Multiple Vendors
Gentoo Linux;
RedHat Fedora Core3, Core2;
SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0;
X.org X11R6 6.7 .0, 6.8, 6.8.1;
XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1
4.3 .0
	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information or cause a Denial of Service.
	Fedora:
	http://download.fedora.redhat.com /pub/fedora/linux/core/updates
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200411-28.xml
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	X.org:
	http://www.x.org/pub/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2004-537.html
	Currently we are not aware of any exploits for these vulnerabilities
		LibXPM Multiple Vulnerabilities
		CVE Name:
		CAN-2004-0914
			Low/
			Medium/
			High
			(Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)
				X.Org Foundation Security Advisory, November 17, 2004
				Fedora Update Notifications, FEDORA-2004-433 & 434, November 17 & 18, 2004
				SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004
				Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004
				Fedora Security Update Notifications FEDORA-2003-464, 465, 466, & 467, December 1, 2004
				RedHat Security Advisory, RHSA-2004:537-17, December 2, 2004

Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8 **SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9**	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/linux-2.6/gnupatch@41925edcVccsXZXObG444GFvEJ94GQ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SUSE:** **http://www.SUSE.de/de/security/2004_42_kernel.html** **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-549.html** Proofs of Concept exploit scripts have been published.	Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities CVE Names: CAN-2004-1070 CAN-2004-1071 CAN-2004-1072 CAN-2004-1073	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 **SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004** **Red Hat Advisory: RHSA-2004:549-10, December 2, 2004**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32; **SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9**	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SUSE:** **http://www.SUSE.de/de/security/2004_42_kernel.html** **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-549.html** Currently we are not aware of any exploits for these vulnerabilities	Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service CVE Names: CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 **SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004** **Red Hat Advisory: RHSA-2004:549-10, December 2, 2004**
Multiple Vendors Linux kernel 2.6.x, 2.4.x , **SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9**	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. **SUSE:** **http://www.SUSE.de/de/security/2004_42_kernel.html** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure CVE Name: CAN-2004-1074	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA13308, November 25, 2004 **SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004**

Multiple Vendors Linux Kernel AMD64/EM64T prior to 2.4.23	A vulnerability exists in the Linux kernel running on AMD's AMD64 and Intel's EM64T which may allow a local malicious user to gain elevated privileges. A local user can exploit a flaw in the setting of TSS limits to cause the system to crash or to potentially gain elevated privileges. A fixed version (2.4.23) is available: www.kernel.org/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel AMD64/EM64T TSS Limit Elevated Privileges CVE Name: CAN-2004-0812	Medium	Red Hat Advisory: RHSA-2004:549-10, December 2, 2004
Multiple Vendors Linux Kernel USB Driver prior to 2.4.27	A vulnerability exists in certain USB drivers because uninitialized structures are used and then 'copy_to_user(...)' kernel calls are made from these structures, which could let a malicious user obtain obtain uninitialized kernel memory contents. Update available at: http://kernel.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-24.xml Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-549.html** We are not aware of any exploits for this vulnerability.	Linux Kernel USB Driver Kernel Memory CVE Name: CAN-2004-0685	Medium	US-CERT Vulnerability Note VU#981134, October 25, 2004 **RedHat Security Advisory, December 2, 2004**
Multiple Vendors LVM Logical Volume Management Utilities 1.0.4, 1.0.7, 1.0.8	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lvm10/ Debian: http://security.debian.org/pool/updates/main/l/lvm10/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-22.xml **Mandrakesoft:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:144** There is no exploit code required.	Multiple Vendors Trustix LVM Utilities Insecure Temporary File Creation CVE Name: CAN-2004-0972	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Ubuntu Security Notice, USN-15-1, November 1, 2004 Debian Security Advisory, DSA 583-1, November 3, 2004 Gentoo Linux Security Advisory, GLSA 200411-22, November 11, 2004 **Mandrakesoft Security Advisory, MDKSA-2004:144, December 6, 2004**
Nicolas Rougier gnubiff	A remote malicious user can send unterminated lines, an unterminated response to the IMAP SELECT, SEARCH, and FETCH commands, or an unterminated response to the POP3 TOP command to cause Denial of Service conditions. The vendor has released a fixed version (2.0.3), available at: http://sourceforge.net/project/showfiles.php?group_id=94176 Currently we are not aware of any exploits for this vulnerability.	Nicolas Rougier gnubiff Denial of Service	Low	SecurityTracker Alert ID: 1012367, December 1, 2004
Open Group Open Motif 2.x, Motif 1.x	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-537.html Currently we are not aware of any exploits for these vulnerabilities.	Open Group Motif / Open Motif libXpm Vulnerabilities CVE Names: CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Solutions Secunia Advisory ID: SA13353, December 2, 2004 RedHat Security Advisory: RHSA-2004:537-17, December 2, 2004
OpenSSL Project OpenSSL 0.9.6, 0.9.6 a-0.9.6 m, 0.9.7c	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ **Debian:** **http://www.debian.org/security/2004/dsa-603** **Mandrakesoft:** **http://www.mandrakesoft.com/security/**	OpenSSL Insecure Temporary File Creation CVE Name: CAN-2004-0975	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200411-15, November 8, 2004 Ubuntu Security Notice, USN-24-1, November 11, 2004 **Debian Security Advisory DSA-603-1, December 1, 2004**

	advisories?name=MDKSA-2004:147 There is no exploit code required.			**Mandrakesoft Security Advisory, MDKSA-2004:147, December 6, 2004**
PHP Arena paFileDB 3.1	Multiple vulnerabilities exists that could allow a remote malicious user to view the administrator's hashed password and determine the installation path. If the 'sessions' method is used, a remote user can access the sessions directory and, if the administrator is logged in, view the administrator's hashed password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHP Arena paFileDB Hashed Passwords Access	Medium	SecurityTracker Alert ID: 1012421, December 3, 2004
phpMyAdmin Development Team phpMyAdmin 2.5 .0-2.5.7, 2.6 .0pl1&2	Multiple Cross-Site Scripting vulnerabilities exist: a vulnerability exists in 'config.inc.php' if the 'PmaAbsoluteUri' parameter is not set, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'read_dump.php' due to insufficient validation of the 'zero_rows' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to insufficient validation of inputs on the confirm page, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/ phpmyadmin/phpMyAdmin-2.6.0-pl3.tar.gz?download **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-36.xml** Proofs of Concept exploits have been published.	PHPMyAdmin Multiple Remote Cross-Site Scripting	High	netVigilance Security Advisory 5, November 19, 2004 **Gentoo Linux Security Advisory, GLSA 200411-36, November 27, 2004**
pizzashack.org rssh 2.2.2	A vulnerability exists which can be exploited to bypass certain security restrictions. The problem is that some of the predefined applications support flags, which allows command execution. This can be exploited to bypass the shell restriction and execute arbitrary commands. Gentoo: http://security.gentoo.org/glsa/glsa-200412-01.xml Currently we are not aware of any exploits for this vulnerability.	pizzashack rssh Security Bypass	High	Secunia Advisory ID: SA13363, December 3, 2004 Gentoo Linux Security Advisory, GLSA 200412-01 / scponly, December 3, 2004
PNG Development Group Conectiva Debian Fedora Gentoo Mandrakesoft RedHat SUSE Sun Solaris HP-UX GraphicsMagick ImageMagick Slackware libpng 1.2.5 and 1.0.15	Multiple vulnerabilities exist in the libpng library which could allow a remote malicious user to crash or execute arbitrary code on an affected system. These vulnerabilities include: • libpng fails to properly check length of transparency chunk (tRNS) data, • libpng png_handle_iCCP() NULL pointer dereference, • libpng integer overflow in image height processing, • libpng png_handle_sPLT() integer overflow, • libpng png_handle_sBIT() performs insufficient bounds checking, • libpng contains integer overflows in progressive display image reading. If using original, update to libpng version 1.2.6rc1 (release candidate 1) available at: http://www.libpng.org/pub/png/libpng.html Conectiva: http://distro.conectiva.com.br/atualizacoes/ index.php?id=a&anuncio=000856 Debian: http://lists.debian.org/debian-security-announce/ debian-security-announce-2004/msg00139.html Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml Mandrakesoft: http://www.mandrakesoft.com/security/advisories ?name=MDKSA-2004:079 RedHat http://rhn.redhat.com/ SUSE: http://www.SUSE.de/de/security/2004_23_libpng.html Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/2/ Sun Solaris: http://sunsolve.sun.com/pub-cgi/ retrieve.pl?doc=fsalert/57617 HP-UX: http://www4.itrc.hp.com/service/cki/doc Display.do?docId=HPSBUX01065 GraphicsMagick: http://www.graphicsmagick.org/ www/download.html ImageMagick:	Multiple Vulnerabilities in libpng CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599	High	US-CERT Technical Cyber Security Alert TA04-217A, August 4, 2004 US-CERT Vulnerability Notes VU#160448, VU#388984, VU#817368, VU#236656, VU#477512, VU#286464, August 4, 2004 SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004 SCO Security Advisory, SCOSA-2004.16, October 12, 2004 Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004 **Sun(sm) Alert Notification, 57683, November 30, 2004**

	http://www.imagemagick.org/www/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243 Yahoo: http://messenger.yahoo.com/ SUSE: ftp://ftp.SUSE.com/pub/SUSE SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.16 Fedora Legacy: http://download.fedoralegacy.org/redhat/ **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57683-1** A Proof of Concept exploit has been published.			
Red Hat Linux kernel-2.4.20-8.athlon.rpm, 2.4.20-8.i386.rpm, 2.4.20-8.i586.rpm, 2.4.20-8.i686.rpm, kernel-smp-2.4.20-8.athlon.rpm, kernel-smp-2.4.20-8.i586.rpm , kernel-smp-2.4.20-8.i686.rpm , kernel-source-2.4.20-8.i386.rpm, Linux 8.0, i686, i386	A buffer overflow vulnerability exists in the 'ubsec_keysetup()' function in '/drivers/crypto/bcm/pkey.c,' which could let a malicious user cause a Denial of Service or possibly execute arbitrary code. **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-549.html** Currently we are not aware of any exploits for this vulnerability.	Red Hat BCM5820 Linux Driver Buffer Overflow CVE Name: CAN-2004-0619	High/Low (High if arbitrary code can be executed; and Low if a DoS)	SecurityTracker Alert, 1010575, June 24, 2004 **Red Hat Advisory: RHSA-2004:549-10, December 2, 2004**
Sandino Flores Moreno Gaim Festival Plug-in 0.68, 0.68.2, 0.70, 0.71, 0.76, 0.77, 0.78, 0.81, 1.0	A remote Denial of Service vulnerability exists because the plug-in does not handle certain characters correctly. There is no exploit code required. Currently we are not aware of any exploits for this vulnerability.	Sandino Flores Moreno Gaim Festival Plug-in Remote Denial of Service	Low	SecurityFocus, December 3, 2004
Sublimation scponly prior to 4.0	A vulnerability exists which can be exploited to bypass certain security restrictions. The problem is that some of the predefined applications support flags, which allows command execution. This can be exploited to bypass the shell restriction and execute arbitrary commands. Updates available at: http://www.sublimation.org/scponly/#download Gentoo: http://security.gentoo.org/glsa/glsa-200412-01.xml Currently we are not aware of any exploits for this vulnerability.	Sublimation scponly Security Bypass	High	Bugtraq, December 2, 2004 Gentoo Linux Security Advisory, GLSA 200412-01 / scponly, December 3, 2004
Sun Microsystems Sun Solaris 7, 8, 9	There is a buffer overflow vulnerability in the ping(1M) command that could allow a local malicious user obtain elevated privileges. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57675-1 As a workaround, Sun indicates that you can remove the set user id (setuid) bit: # chmod u-s /usr/sbin/ping Currently we are not aware of any exploits for this vulnerability.	Sun Solaris 'ping' Buffer Overflow	Medium	Sun Alert Notification 57675, November 30, 2004
SUSE SUSE Linux 9.1 and SUSE Linux Enterprise Server 9	There is a vulnerability in the evolution SSL certificate handling which leads to untrusted certificates. Update: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE evolution SSL Handling	Medium	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004
SUSE All SUSE Linux based products	Several protocol handlers in the network analysis tool ethereal have security problems which could lead bad network input to ethereal crashing. Update: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE ethereal Denial of Service CVE Names: CAN-2004-0504 CAN-2004-0505 CAN-2004-0506 CAN-2004-0507	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004
SUSE All SUSE Linux based products	Several GNOME vfs handlers had problematic code, for instance unsafe argument evaluation and similar. Update: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE GNOME Input Validation	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004

SUSE Linux 9.1, Linux Enterprise Server 9	A vulnerability exists because a malicious user can send commands to SCSI devices, which potentially results in the failure of the targeted device to further operate. This may result in the permanent, unrecoverable destruction of SCSI devices, requiring that they be sent to the vendor for service or replacement. Update available at: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE Linux Kernel Unauthorized SCSI Command	Medium	SUSE Security Announcement, SUSE-SA:2004:042, December 1, 2004
SUSE Linux Enterprise Server 9	A remote Denial of Service and storage corruption vulnerability exists due to a memory corruption in the NFS 'readdirplus' command. Update available at: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE Linux Enterprise Server NFS Remote Denial Of Service & Storage Corruption	Low/ Medium (Medium if data is corrupted)	SUSE Security Announcement, SUSE-SA:2004:042, December 1, 2004
SUSE SUSE Linux 8.1 and SUSE Linux Enterprise Server 8	A buffer overflow fix in the resolver libraries of glibc 2.2 was found missing. Update: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE glibc Buffer Overflow CVE Name: CAN-2002-0029	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004
SUSE SUSE Linux 8.2 up to 9.2, and SUSE Linux Enterprise Server 9	There is a vulnerability in resmgr which is used for handling permissions of normal desktop based devices (audio, video, USB, and similar). It was possible for a remotely logged in malicious user to gain access to the virtual desktop group through resmgr indirectly gaining access to the desktop devices. Update: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE resmgr Access	Medium	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004
Trustix file 4.11 and prior (Trustix)	A vulnerability exists in the ELF header parsing code in 'file'. A malicious user may be able to create a specially crafted ELF file that, when processed using 'file', may be able to modify the stack and potentially execute arbitrary code. Update to version 4.12: ftp://ftp.astron.com/pub/file/ Currently we are not aware of any exploits for this vulnerability.	Trustix 'File' Processing ELF Headers Stack Overflow	High	Trustix Secure Linux Advisory #2004-0063, November 26, 2004

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Albrecht Guenther PHProjekt 2.0, 2.0.1, 2.1 a, 2.1-2.4, 3.0-3.2, 4.2	A vulnerability exists in 'setup.php' because arbitrary PHP scripts can be uploaded, including operating system commands, which could let a remote malicious user modify the configuration and execute arbitrary scripts. Patch available at: http://phprojekt.com/files/4.2/setup.zip Currently we are not aware of any exploits for this vulnerability.	PHProjekt 'setup.php' File Upload	High	Secunia Advisory, SA13355, December 2, 2004
Apache Software Foundation Jakarta Lucene 1.4.2	A Cross-Site Scripting vulnerability exists in the SP demo page (src/jsp/results.jsp) due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.apache.org/dyn/closer.cgi/jakarta/lucene/ There is no exploit code required.	Apache Jakarta Results.JSP Remote Cross-Site Scripting	High	SecurityFocus, December 3, 2004
Cisco Systems, 2650 Multiservice Platform, 2650XM Multiservice Platform, 2651 Multiservice Platform, 2651XM Multiservice Platform, Cisco 7200, 7300, 7500, 7600, Catalyst 7600 Sup720/MSFC3, IOS 12.2 (18)SW, 12.2 (18)SV, 12.2 (18)SE, 12.2 (18)S,12.2 (18)EWA, 12.2 (18)EW, 12.2 (14)SZ	A remote Denial of Service vulnerability exists when a malicious user submits specially crafted DHCP packets that will remain in the queue. **Updated Software version table - 12.2(20)EW.** Updates and workarounds available at: http://www.cisco.com/warp/public/707/ cisco-sa-20041110-dhcp.shtml An exploit script is not required.	Cisco IOS DHCP Input Queue Blocking Remote Denial of Service	Low	Cisco Security Advisory, 63312, November 10, 2004 US-CERT Vulnerability Note VU#630104, November 11, 2004 Technical Cyber Security Alert, TA04-316A, November 11, 2004 **Cisco Security Advisory, 63312, Rev. 1.2, December 1, 2004**
FreeImage FreeImage 3.0.0-3.0.4, 3.1 .0, 3.2 .0, 3.2.1, 3.3.0, 3.4 .0, 3.5 .0	A buffer overflow vulnerability exists when processing ILBM (InterLeaved BitMap) images, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/	FreeImage Interleaved Bitmap Image Buffer Overflow	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA13331, November 30, 2004

	freeimage/FreeImage351.zip?download Currently we are not aware of any exploits for this vulnerability.			
Hitachi Groupmax World Wide Web 03-11-/B, 03-10-/H, 03-00, 02-31-/I, 02-20-/A, 02-20, 02-00, World Wide Web Desktop 06-52-/B, 06-52, 06-51-/C, 06-51-/B, 06-51, 06-50-/C, 06-50-/B, 06-00, 05-11-/J, 05-11-/I, 05-11-/F, 05-00, World Wide Web Desktop for Jichitai 06-52, 06-51	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of 'QUERY' before being returned to users, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability exists due to insufficient input validation when handling template names, which could let a remote malicious user obtain sensitive information. Update information available at: http://www.hitachi-support.com/ security_e/vuls_e/HS04-007_e/01-e.html There is no exploit code required.	Groupmax World Wide Web Cross-Site Scripting & Directory Traversal	Medium/ High (High if arbitrary code can be executed)	Hitachi Security Advisory, HS04-007, November 29, 2004
IBM WebSphere Commerce 5.x	A vulnerability exists if store views update the database or directly invoke commands that perform the database update, which could let a remote malicious user obtain sensitive information. WebSphere Commerce fixes can be obtained by contacting the vendor. Currently we are not aware of any exploits for this vulnerability.	IBM WebSphere Commerce Default User Information Disclosure	Medium	Secunia Advisory, SA13234, December 3, 2004
Multiple Vendors Archive::Zip 1.13, F-Secure Anti-Virus for Microsoft Exchange 6.30, 6.30 SR1, and 6.31, Computer Associates, Eset, Kaspersky, McAfee, Sophos, RAV	Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows malicious users to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. Instructions for Computer Associates, Eset, Kaspersky, McAfee, Sophos, and RAV are available at: http://www.idefense.com/application/poi/display?id =153&type=vulnerabilities&flashstatus=true Gentoo: http://security.gentoo.org/glsa/glsa-200410-31.xml Mandrakelinux 10.1 and Mandrakelinux 10.1/X86_64: http://www.mandrakesoft.com/security/advisories A fix for F-Secure is available at:: ftp://ftp.f-secure.com/support/ hotfix/fsav-mse/fsavmse63x-02.zip **SUSE:** **http://www.SUSE.com/en/private/ download/updates/92_i386.html** A Proof of Concept exploit script has been published.	Multiple Vendor Anti-Virus Software Detection Evasion CVE Names: CAN-2004-0932 CAN-2004-0933 CAN-2004-0934 CAN-2004-0935 CAN-2004-0936 CAN-2004-0937	High	iDEFENSE Security Advisory, October 18, 2004 Secunia Advisory ID: SA13038, November 1, 2004 SecurityFocus, Bugtraq ID: 11448, November 2, 2004 SecurityTracker Alert ID: 1012057, November 3, 2004 SecurityFocus, November 15, 2004 **SecurityFocus, November 29, 2004**
Novell NetMail 3.x	A vulnerability exists because the NMAP (Network Messaging Application Protocol) authentication credential is set automatically during installation and not changed after the installation has finished, which could let a remote malicious user obtain access to the mail store data with read/write permissions or send unauthorized messages. Novell indicates that you should use the NMAP Server Credential Generator (nmapcred) to set a unique NMAP authentication credential. Currently we are not aware of any exploits for this vulnerability.	Novell NetMail Default Authentication Credentials	Medium	Secunia Advisory, SA13377, December 6, 2004
S9Y Serendipity 0.3, 0.4, 0.5-pl1, 0.5, 0.6 -rc1&2, 0.6 -pl1-13, 0.6, 0.7 -rc1, 0.7 -beta1-beta4, 0.7	A Cross-Site Scripting vulnerability exists in 'compat.php' due to insufficient sanitization of the 'searchTerm parameter, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://prdownloads.sourceforge.net/php-blog/serendipity-0.7.1.tar.gz?download There is no exploit code required.	S9Y Serendipity Remote Cross-Site Scripting	High	SecurityTracker Alert ID, 1012383, December 2, 2004
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/ squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml **Conectiva:** **ftp://atualizacoes.conectiva.com.br/9** **Fedora: http://download.fedora.redhat. com/pub/fedora/linux/core/updates/** An exploit script is not required.	SquirrelMail Cross-Site Scripting CVE Name: CAN-2004-1036	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 **Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004** **Conectiva Linux Security Announcement, CLA-2004:905,**

				December 2, 2004
SugarCRM Inc. SurgarCRM 2.5 & prior	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient validation of the 'record' variable, which could let a remote malicious user inject arbitrary SQL commands; and a vulnerability exists which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	SugarCRM Multiple Input Validation	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1012373, December 2, 2004
Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; Conectiva Linux 10.0; **Gentoo Linux; HP HP-UX B.11.23, B.11.22, B.11.11, B.11.00, HP Java SDK/RTE for HP-UX PA-RISC 1.3, HP Java SDK/RTE for HP-UX PA-RISC 1.4**	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-38.xml** **HP:** **http://www.hp.com/go/java** Currently we are not aware of any exploits for this vulnerability.	Sun Java Plug-in Sandbox Security Bypass CVE Name: CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT Vulnerability Note, VU#760344, November 23, 2004 Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004 **Gentoo Linux Security Advisory, GLSA 200411-38, November 29, 2004** HP Security Bulletin, HPSBUX01100, December 1, 2004
ViewCVS ViewCVS 0.9.2 & prior	A vulnerability exists because it is possible to access CVSROOT and forbidden directories via the tarball generation functionality, which could let malicious user bypass security restrictions. Debian: http://security.debian.org/pool/updates/main/v/viewcvs/ Currently we are not aware of any exploits for this vulnerability.	ViewCVS Ignores 'hide_cvsroot' and 'forbidden' Settings	Medium	SecurityTracker Alert ID, 1012431, December 6, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
December 7, 2004	stripwire-1.1.tar.gz	N/A	A tool which demonstrates vulnerabilities in md5 checks.
December 2, 2004	kreedexec.zip	No	Exploit for the Burut Kreed Game Server Multiple Remote vulnerabilities.
December 1, 2004	mercury.py ex_MERCURY.c ex_MERCURY2.c	Yes	Scripps that exploit the Mercury Mail Multiple Remote IMAP Stack Buffer Overflow vulnerabilities.
November 30, 2004	janados.zip	Yes	Exploit for the JanaServer 2 Multiple Remote Denial of Service vulnerabilities.
November 30, 2004	WeBrute	N/A	A Brute Forcing tool to discover hidden directories, files or parameters in the URL # of a webserver.
November 30, 2004	WS_FTP_Overflow.pl ws_ftpOverflowExploitByNoPh0BiA.c	No	Scripts that exploit the IpSwitch WS_FTP Buffer Overflow vulnerability.

[back to top]

Trends

- MessageLabs Publishes 2004 Email Security Trends and 2005 Predictions Report.
  - The report found that phishing-related online identity theft has established itself as the principal threat of 2004 and may signal the beginning of a wave of email attacks targeted at individuals and small groups of companies.
  - Spam and virus ratios also rose over the last 12 months. During the year, the virus infection average ratio was 1 in 16, compared to 2003 when it was 1 in 33.
  - Recent evidence also suggests that Trojans and other malicious code have been developed during 2004 specifically to compromise particular organizations. Tailored malicious activity ranging from blackmailing online gaming sites with Denial of Service (DoS) attacks to threats to send out child pornography in the name of a particular organization.

- For more information, see: http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=1245&region=

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-D	Win32 Worm	Slight Increase	March 2004
3	Zafi-B	Win32 Worm	Slight Decrease	June 2004
4	Bagle-AT	Win32 Worm	Decrease	October 2004
5	Sober-I	Win32 Worm	New to Table	November 2004
6	Netsky-Z	Win32 Worm	Decrease	April 2004
7	Netsky-Q	Win32 Worm	Increase	March 2004
8	Bagle-AA	Win32 Worm	Decrease	April 2004
9	Bagle-AU	Win32 Worm	New to Table	October 2004
10	Netsky-B	Win32 Worm	Decrease	February 2004

Table Updated December 6, 2004

Viruses or Trojans Considered to be a High Level of Threat

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Agobot-OL	WORM_AGOBOT.ACE W32/Gaobot.worm.gen.q Backdoor.Win32.Agobot.gen	Win32 Worm
HTML_IFRAMEBOF.B		HTML Virus
I-Worm.Lovgate.ad	W32/Lovgate.ah@MM W32.Lovgate.AD@mm Win32.HLLM.MyDoom.based W32/Lovgate-F Win32/Lovgate.AH@mm Worm/Lovgate.AD W32/Lovgate.AK@mm Win32:Lovgate-AK I-Worm/Lovgate Win32.LovGate.AC@mm Worm.Lovgate.AC W32/Lovgate.AO Win32/Lovgate.AK (Eset)	Win32 Worm
I-Worm.Mabutu.a	W32/Mabutu.a@MM W32.Mota.B@mm Win32.HLLM.Mabutu W32/Mabutu-A Win32/Mabutu.A@mm Worm/Mabutu.A W32/Mabuto.B@mm Win32:Mabutu-Dll I-Worm/Mabutu.A Win32.Mabutu.B@mm Worm.Mabutu.A.3 W32/Mabutu.A.worm Win32/Mabutu.A	Win32 Worm
JS.Kidrash		JavaScript Virus
PWS-Banker.d		Trojan
PWSteal.Tarno.K		Trojan
QLowZones-4		Trojan
Troj/Agent-BF	Trojan-Downloader.Win32.Agent.ea	Trojan
Troj/Banker-BG		Trojan
Trojan.Frutca		Trojan

Trojan.Wlogo		Trojan
W32.Aidid		Win32 Virus
W32.Atak.B@mm		Win32 Worm
W32.Beagle@mm!enc		Win32 Worm
W32.Salga.A@mm	W32/Salga.a@MM	Win32 Worm
W32.Setclo	W32/Setclo.worm	Win32 Worm
W32/Agobot-NZ	Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Agobot-OH	DOS_AGOBOT.GEN Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Atak-E		Win32 Worm
W32/Rbot-QX	WORM_RBOT.XQ Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.j	Win32 Worm
W32/Rbot-RC	WORM_SDBOT.AFI Backdoor.Win32.Rbot.dy	Win32 Worm
W32/Rbot-RE		Win32 Worm
W32/Rbot-RF		Win32 Worm
W32/Sdbot-RU	W32/Sdbot.worm.gen Win32.IRCBot.a	Win32 Worm
W32/Wurmark-A	Email-Worm.Win32.Wurmark.a W32/Mugly.b@MM	Win32 Worm
Win32.Fuzzorin	TROJ_AGENT.GG Generic BackDoor.p Win32.Fuzzorin.A Win32/Fuzzorin.A.Trojan Win32.Fuzzorin.B Win32.Fuzzorin.C Win32.Fuzzorin.D W32/SillyTrojan.N@bd Trojan.Win32.Helodor.a	Trojan
Win32.Orpheus.A	W32/Hpl.worm.dll W32.Orpheus.A WORM_ORPHEUS.A Worm.Win32.Orpheus.a	Win32 Worm
Win32.Yanz.A	Win32/Yaha.Variant.Worm I-Worm.Yanz.a WORM_YANZ.A Yanz.A@mm W32/Yanz-A W32/Yanzi.A@mm	Win32 Worm
WORM_ATAK.D	I-Worm/Atak.C W32/Atak.d@MM W32/Atak-D W32/Atak.D.worm	Internet Worm
WORM_RBOT.ADD		Internet Worm

[back to top]

Last updated December 08, 2004